UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

KATHERINE PETILLO, on behalf of herself and all others similarly situated, Plaintiff, v. DILIGENT CORPORATION, and UNIVERSITY OF COLORADO HEALTH dba UC HEALTH, Defendant.	Case No. 23-cv-2439 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff, Katherine Petillo, through her attorneys, bring this Class Action Complaint against the Defendants, Diligent Corporation ("Diligent") and University of Colorado Health d/b/a UC Health ("UC Health") (collectively, "Defendants"), alleging as follows:

INTRODUCTION

1. Diligent, a software-as-a-service company serving corporate boards across the country, lost control over its client's consumers' highly sensitive personal information in a September 30, 2022, data breach by cybercriminals ("Data Breach"). On information and belief, the Data Breach affected over 48,000 individuals.[1]

2. On information and belief, the Data Breach began on or around September 30, 2022, when an unauthorized party gained access to Diligent's network, and was not discovered by Diligent's "security team" until almost two months later, on November 11, 2022. Following an internal investigation, Diligent learned cybercriminals gained unauthorized access to its client's consumers' personally identifiable information ("PII") and private health information ("PHI"). PII

[1] Health IT Security, UC Health Data Breaches, https://healthitsecurity.com/news/uchealth-ucla-health-report-healthcare-data-breaches (last visited March 16, 2023).

and PHI is collectively referred to as "Sensitive Information."

3. On information and belief, cybercriminals bypassed Diligent's inadequate security systems to access consumers' Sensitive Information in its computer systems.

4. On or around November 11, 2022, UC Health, a health care system and a client of Diligent, was first notified by Diligent that its patients' Sensitive Information were involved in the Data Breach.

5. On or about January 27, 2023 –four months after the unauthorized party first gained access to consumers' Sensitive Information and over two months after Defendants first discovered the Data Breach – UC Health finally notified Class Members about the Data Breach ("Breach Notice") which is attached as **Exhibit A**.

6. UC Health's Breach Notice obfuscated the nature of the breach and the threat it posed—refusing to tell its patients how many people were impacted, how the breach happened, or why it took UC Health two months to begin notifying victims that hackers had gained access to highly private Sensitive Information.

7. Defendants' failure to timely detect and report the Data Breach made its consumers vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Sensitive Information.

8. Defendants knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII and PHI misuse.

9. In failing to adequately protect Plaintiff's and the Class's Sensitive Information, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendants violated state and federal law and harmed an unknown number of its current and

former consumers and patients.

10. Plaintiff and members of the proposed Class are victims of Defendants' negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendants with their Sensitive Information. But Defendants betrayed that trust. Defendants failed to properly use up-to-date security practices to prevent the Data Breach.

11. Plaintiff Katherine Petillo is a Data Breach victim.

12. Accordingly, Plaintiff, on her own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendants' possession.

PARTIES

13. Plaintiff, Katherine Petillo, is a natural person and citizen of Colorado, residing in Denver, Colorado, where she intends to remain. Plaintiff Petillo is a Data Breach victim, receiving the Breach Notice on February 28, 2023.

14. Defendant, Diligent, is a New York Corporation, with its principal place of business at 111 W 33rd St 16th Floor, New York, NY 10001.

15. Defendant, UC Health, is a Colorado Corporation, with its principal place of business at 12401 East 17th Ave., Mail Stop F417, Aurora, CO 80045.

JURISDICTION & VENUE

16. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and Plaintiff and at least one Defendant are citizens of different states.

17. This Court has personal jurisdiction over Defendants because at least one Defendant maintains its principal place of business this District and does substantial business in this District.

18. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

BACKGROUND FACTS

Diligent

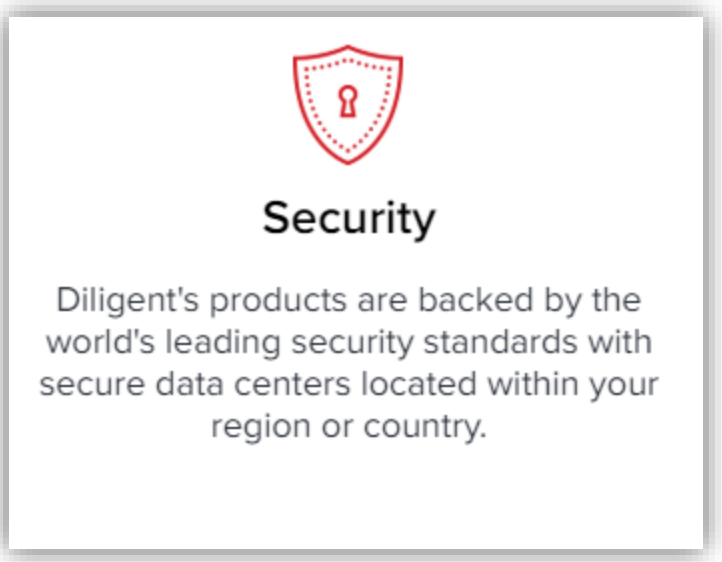
19. Diligent is a "SaaS" company that provides management software to corporate boards. Holding itself out as the "#1 Global Board Meeting Software." Diligent boasts a total revenue of 250 million. [2]

20. Diligent's software services are specialized for corporations, government organizations and healthcare providers who manage highly sensitive data. Diligent thus must oversee, manage, and protect the Sensitive Information of its clients' consumers.

21. On information and belief, these third-party consumers, whose Sensitive Information was collected by Diligent, do not do any business with Diligent.

22. In working with third party consumers' highly sensitive data, Diligent advertises that it employs the "world's leading security standards"[3] to protect information stored on its systems:

[2] Zoominfo, Diligent, https://www.zoominfo.com/c/diligent-corp/18236665 (last visited March 16, 2023).
[3] Diligent, Diligent's landing page, https://www.diligent.com/landing/solutions/lp-board-portal-demo/?&utm_source=google&utm_medium=cpc&_bt=611705541966&_bk=diligent%20corporation&_bm=b&_bn=g&gclid=CjwKCAjw6MKXBhA5EiwANWLODLEKe17KlKrUU0AwTofmfF135LImmeZWupSe_KQ2sCTJRh4ScR-0MRoCCOUQAvD_BwE&gclsrc=aw.ds (last visited March 16, 2023).



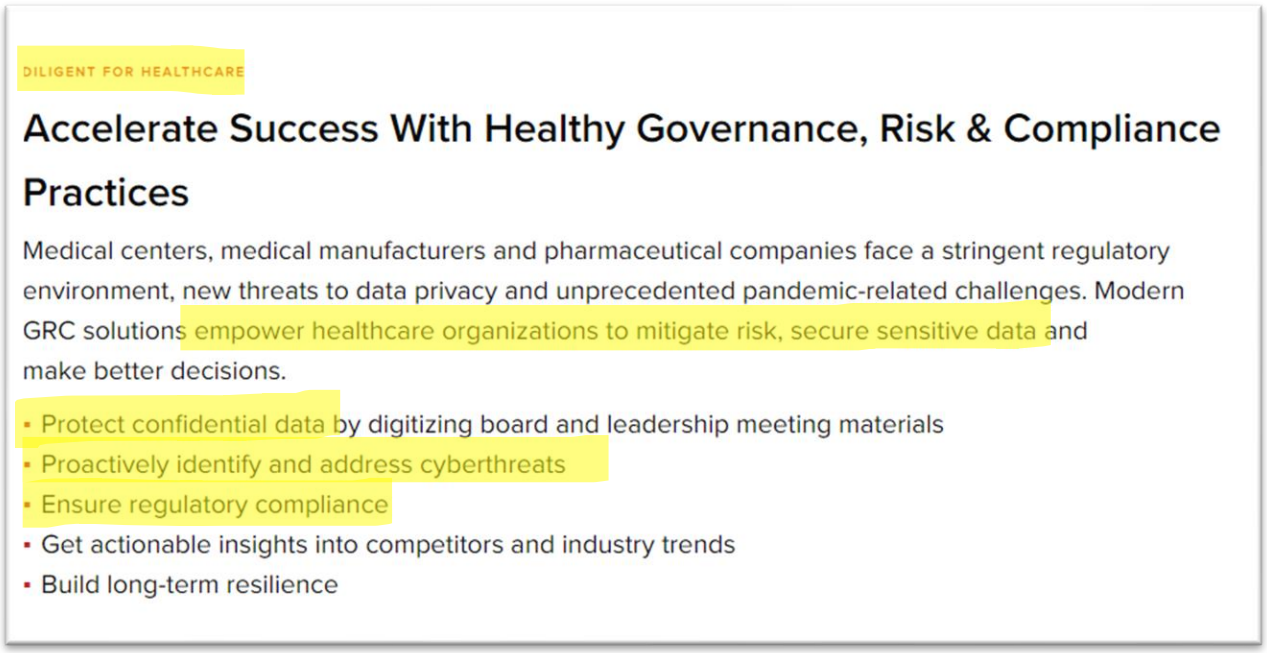
23. It also claims to consult on cybersecurity for its clients, using cybersecurity "scorecards" that grade a company's security systems.[4]

24. As a self-proclaimed "world leader" in cybersecurity company that handles highly sensitive aspects of its clients' business, Diligent understood the need to protect its client's consumers' data and prioritize its data security. In fact, in 2017, Diligent warned that "with [the] increase of hacking activity around the world, user data has become more valuable and is become [*sic*] a viable form of currency for hackers." Because of this increase in hacking activity, Diligent denounced cloud storage drawbacks and insisted that "Diligent Boards [are] the Solution."[5]

25. Additionally, Diligent also presents itself as a leading authority in the healthcare

[4] SecurityScorecard's website article announcing its partnership with Diligent at https://securityscorecard.com/company/press/diligent-delivers-cyber-risk-scores-directly-to-board-directors (last visited March 15, 2023).
[5] Diligent, Cloud Storage Hack, https://www.diligent.com/en-gb/blog/4-reasons-why-some-cloud-storage-solutions-are-not-secure/ (last visited March 15, 2023).

sector, boasting solutions that "empower healthcare organizations to mitigate risk, secure sensitive data and make better decisions." [6]



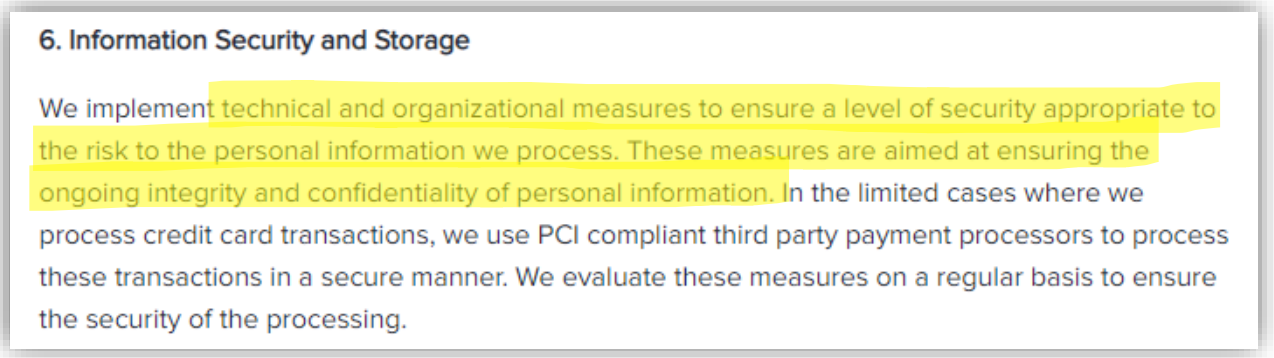
DILIGENT FOR HEALTHCARE

Accelerate Success With Healthy Governance, Risk & Compliance Practices

Medical centers, medical manufacturers and pharmaceutical companies face a stringent regulatory environment, new threats to data privacy and unprecedented pandemic-related challenges. Modern GRC solutions empower healthcare organizations to mitigate risk, secure sensitive data and make better decisions.

- Protect confidential data by digitizing board and leadership meeting materials
- Proactively identify and address cyberthreats
- Ensure regulatory compliance
- Get actionable insights into competitors and industry trends
- Build long-term resilience

26. Diligent's privacy policy also promises to protect all Sensitive Information it collects by using "a level of security appropriate to the risk to the personal information we process."[7]



6. Information Security and Storage

We implement technical and organizational measures to ensure a level of security appropriate to the risk to the personal information we process. These measures are aimed at ensuring the ongoing integrity and confidentiality of personal information. In the limited cases where we process credit card transactions, we use PCI compliant third party payment processors to process these transactions in a secure manner. We evaluate these measures on a regular basis to ensure the security of the processing.

27. But, on information and belief, Diligent fails to strictly adhere to these policies in maintaining its client's consumers' Sensitive Information.

[6] Diligent, Diligent for Healthcare, https://www.diligent.com/industries/healthcare/ (last visited March 16, 2023).
[7] Diligent's privacy policy at https://www.diligent.com/privacy/ (last visited March 16, 2023).

UC Health

28. On information and belief, UC Health is a healthcare system headquartered in Colorado, providing healthcare services. According to its website, UC Health "[builds] a team of exceptional people… who consistently do what is right for the individuals we are honored to serve."[8] UC Health boasts a total revenue of 5.4 billion. [9]

29. In its privacy policy, UC Health promises that it "values your privacy and confidentiality of the information you choose to share." [10]

30. As part of its business, UC Health receives and maintains the Sensitive Information of thousands of current and former patients. In doing so, UC Health implicitly promises to safeguard their Sensitive Information.

31. In collecting and maintaining its current and former patients' Sensitive Information, UC Health agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their Sensitive Information

32. Despite recognizing its duty to do so, on information and belief, UC Health has not implemented reasonable cybersecurity safeguards or policies to protect its patients' Sensitive Information or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, UC Health leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to patients' Sensitive Information.

[8] UC health, about UC Health, https://www.uchealth.org/about/ (last visited March 16, 2023).
[9] Zoominfo, UC Health, https://www.zoominfo.com/c/university-of-colorado-health/355889766 (last visited March 16, 2023).
[10] UC Helath, Privacy Policy, https://www.uchealth.org/privacy-policy/#:~:text=UCHealth%20may%20use%20your%20precise,UCHealth%20website%20or%20mobile%20application. (last visited March 16, 2023).

The Data Breach

33. Plaintiff is a patient of UC Health. As a condition of treatment with UC Health, Plaintiff provided UC Health with her Sensitive Information, including but not limited to her name, address, date of birth, Social Security number, and health insurance information. UC Health used that Sensitive Information to facilitate its treatment of Plaintiff and required Plaintiff to provide that Sensitive Information to obtain treatment and care.

34. On information and belief, Diligent got Plaintiff's information through UC Health, who provided Diligent with Plaintiff's Sensitive Information including but not limited to her name, address, Social Security Number, date of birth, medical treatment information, and health insurance information.

35. On information and belief, Defendants collect and maintains consumers' Sensitive Information in their computer systems.

36. In collecting and maintaining the Sensitive Information, Defendants implicitly agree that they will safeguard the data using reasonable means according to their internal policies and federal law.

37. According to the Breach Notice, Diligent found "a security incident which impacted data on [its] servers," on November 11, 2022, and that "further investigation by Diligent revealed on September 30, 2022, an unknown person accessed and downloaded attachments from Diligent's system that contained information about UC Health patients, employees, and providers." Exh. A.

38. In other words, Diligent's investigation revealed that its network had been hacked by cybercriminals almost two months before discovery and that, despite touting itself to have "world leading security standards", Defendant's cyber and data security systems were completely

inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of its consumers' highly private Sensitive Information.

39. Additionally, Defendants admitted that Sensitive information was actually stolen during the Data Breach, confessing that the information was not just accessed, but "**downloaded**" from Diligent's system. Exh. A.

40. Diligent did not notify UC Health until November 11, 2022, almost two months after the breach first began.

41. On or around January 27, 2023 – four months after the Breach first occurred and over two months after Defendants first discovered the Breach – UC Health finally notified Class Members about the Data Breach. However, Plaintiff did not receive a Notice Letter from UC Health until February 28, 2023.

42. Despite its duties and alleged commitments to safeguard Sensitive Information, Defendants do not in fact follow industry standard practices in securing consumers' Sensitive Information, as evidenced by the Data Breach.

43. In response to the Data Breach, Defendants contend that Diligent has or will be taking "additional steps to protect their data and prevent this type of attack from happening again" Exh. A. Although Defendants fail to expand on what these alleged "additional steps" are, such steps should have been in place before the Data Breach.

44. Through its Breach Notice, Defendants also recognized the actual imminent harm and injury that flowed from the Data Breach, so they encouraged breach victims to "protect themselves by watching for any suspicious activity or possible identity theft." Exh. A.

45. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's

Sensitive Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

46. Normally, breached entities provide complimentary identity theft and credit monitoring services to their impacted parties. Not these Defendants. Defendants refuse to provide such basic protection services to its victims. Exh. A. Instead, Defendants merely instructed their victims to be alert for "suspicious activities" and advised that if victims "have any questions or need additional information," to call the phone number listed.

47. Because of the Data Breach, Defendants inflicted injuries upon Plaintiff and Class Members. And yet, Defendants have done absolutely nothing to provide Plaintiff and the Class Members with relief for the damages they suffered and will suffer.

48. On information and belief, Defendants failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over their consumers' Sensitive Information. Defendants' negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the Sensitive Information.

The Data Breach was a Foreseeable Risk of which Defendants were on Notice.

49. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

50. In light of recent high profile data breaches at other healthcare partner and provider companies, Defendants knew or should have known that their electronic records and customers' Sensitive Information would be targeted by cybercriminals.

51. In 2021, a record 1,862 data breaches occurred, resulting in approximately

293,927,708 sensitive records being exposed, a 68% increase from 2020.[11] The 330 breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[12]

52. Indeed, cyberattacks against the healthcare industry have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime." [13]

53. Cyberattacks on medical systems and healthcare partner and provider companies like Defendants have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly." [14]

54. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including Diligent and UC Health.

Plaintiff Petillo's Experience

55. Plaintiff Petillo is a UC Health patient.

56. As a condition of treatment with UC Health, Plaintiff provided it with her Sensitive

[11] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited March 13, 2023).
[12] *Id.*
[13] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited March 13, 2023).
[14] Secret Service Warn of Targeted, Law360, https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited March 13, 2023).

Information, including but not limited to her name, address, date of birth, Social Security number, and health insurance information. UC Health used that Sensitive Information to facilitate its treatment of Plaintiff and required Plaintiff to provide that Sensitive Information to obtain treatment and care.

57. Plaintiff is unsure how Diligent got her information, but assumes UC Health provided Diligent with her Sensitive Information, including but not limited to her name, date of birth, address, Social Security Number, medical treatment information and health insurance information.

58. Plaintiff provided her Sensitive Information to Defendants and trusted that they would use reasonable measures to protect it according to their internal policies and state and federal law.

59. Defendants deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to notify her about it for over three months.

60. In fact, following the Data Breach, Plaintiff was notified by her bank regarding a fraudulent purchase. This demonstrates that Plaintiff's information was stolen in the Data Breach has been placed in the hands of cybercriminals.

61. Additionally, Plaintiff also experienced an increase in spam texts and phone calls since the Data Breach, further suggesting that her Sensitive Information has been placed in the hands of cybercriminals.

62. Plaintiff does not recall ever learning that her Sensitive Information was compromised in a data breach incident, other than the breach at issue in this case.

63. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice

of Data Breach, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

64. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff fears for her personal financial security and uncertainty over what Sensitive Information was exposed in the Data Breach.

65. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

66. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Sensitive Information—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

67. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Sensitive Information being placed in the hands of unauthorized third parties and possibly criminals.

68. Plaintiff has a continuing interest in ensuring that her Sensitive Information, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

69. Plaintiff and members of the proposed Class have suffered injury from the misuse of their Sensitive Information that can be directly traced to Defendants.

70. As a result of Defendants' failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost

time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Sensitive Information is used;

b. The diminution in value of their Sensitive Information;

c. The compromise and continuing publication of their Sensitive Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Sensitive Information; and

h. The continued risk to their Sensitive Information, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the Sensitive Information in their possession.

71. Stolen Sensitive Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII alone can be worth up to $1,000.00 depending on the type of information obtained.

72. The value of Plaintiff's and the Class's Sensitive Information on the black market is considerable. Stolen Sensitive Information trades on the black market for years, and criminals frequently post stolen Sensitive Information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

73. It can take victims years to spot identity theft, giving criminals plenty of time to use

that information for cash.

74. One such example of criminals using Sensitive Information for profit is the development of "Fullz" packages.

75. Cyber-criminals can cross-reference two sources of Sensitive Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

76. The development of "Fullz" packages means that stolen Sensitive Information from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Sensitive Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen Sensitive Information is being misused, and that such misuse is fairly traceable to the Data Breach.

77. Defendants disclosed the Sensitive Information of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendants opened up, disclosed, and exposed the Sensitive Information of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Sensitive Information.

78. Defendants' failure to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their Sensitive Information and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendants failed to adhere to FTC guidelines.

79. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendants, should employ to protect against the unlawful exposure of Sensitive Information.

80. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that they keep;

b. properly dispose of Sensitive Information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

81. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

82. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security

measures.

83. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

84. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendants Violated HIPAA

85. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information. [15]

86. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[16]

87. The Data Breach itself resulted from a combination of inadequacies showing Defendants failure to comply with safeguards mandated by HIPAA. Defendants' security failures

[15] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, inter alia: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[16] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendants in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

88. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations.

CLASS ACTION ALLEGATIONS

89. Plaintiff sues on behalf of herself and the proposed nationwide class ("Class") and state subclass ("Subclass"), defined as follows, pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3):

> **Nationwide Class**: All individuals residing in the United States whose Sensitive Information was compromised in the Data Breach.
>
> **Colorado Subclass**: All individuals residing in Colorado whose Sensitive Information was compromised in the Data Breach.

Excluded from the Class are Defendants, their agents, affiliates, parents, subsidiaries, any entity in which Defendants have a controlling interest, any of Defendants' officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

90. Plaintiff reserves the right to amend the class definition.

91. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiff is representative of the Class, consisting of at least 48,000 members, far too many to join in a single action;

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendants' possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendants, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with the Class's interests, and she has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendants had a duty to use reasonable care in safeguarding Plaintiff's and the Class's Sensitive Information;

ii. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendants were negligent in maintaining, protecting, and securing Sensitive Information;

iv. Whether Defendants breached contract promises to safeguard Plaintiff's and the Class's Sensitive Information;

v. Whether Defendants took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendants' Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

92. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

93. Plaintiff realleges all previous paragraphs as if fully set forth below.

94. Plaintiff and members of the Class entrusted their Sensitive Information to Defendants. Defendants owed to Plaintiff and the Class a duty to exercise reasonable care in handling and using the Sensitive Information in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

95. Defendants owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendants' failure to adequately safeguard their Sensitive Information in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that Sensitive Information —just like the Data Breach that ultimately came to pass. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and the Class's Sensitive Information by disclosing and providing access to this information to unauthorized third parties and by failing to properly supervise both the way the

Sensitive Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

96. Defendants owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their Sensitive Information. Defendants also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and the Class to take appropriate measures to protect their Sensitive Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

97. Defendants owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security protocols. Defendants actively sought and obtained Plaintiff's and the Class's Sensitive Information.

98. The risk that unauthorized persons would attempt to gain access to the Sensitive Information and misuse it was foreseeable. Given that Defendants hold vast amounts of Sensitive Information, it was inevitable that unauthorized individuals would attempt to access Defendants' databases containing the Sensitive Information —whether by malware or otherwise.

99. Sensitive Information is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Sensitive Information of Plaintiff and the Class and the importance of exercising reasonable care in handling it.

100. Defendants breached their duties by failing to exercise reasonable care in supervising their employees, agents, contractors, vendors, and suppliers, and in handling and

securing the Sensitive Information of Plaintiff and the Class which actually and proximately caused the Data Breach and Plaintiff's and the Class's injury. Defendants further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiff and the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

101. Defendants' breach of their common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Sensitive Information by criminals, improper disclosure of their Sensitive Information, lost benefit of their bargain, lost value of their Sensitive Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendants' negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

102. Plaintiff realleges all previous paragraphs as if fully set forth below.

103. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class's Sensitive Information.

104. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce,"

including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect customers or, in this case, consumers' and patients' Sensitive Information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect Plaintiff's and the members of the Class's Sensitive Information.

105. Defendants breached their respective duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Sensitive Information.

106. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and their consumers, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendants were in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

107. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

108. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Sensitive Information.

109. Defendants violated its duty under Section 5 of the FTC Act by failing to use

reasonable measures to protect Plaintiff's and the Class's Sensitive Information and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendants collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

110. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

111. Defendants violated their duty under HIPAA by failing to use reasonable measures to protect their PHI and by not complying with applicable regulations detailed supra. Here too, Defendants' conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendants collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

112. But for Defendants' wrongful and negligent breach of the duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

113. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties and that their breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their Sensitive Information.

114. Had Plaintiff and the Class known that Defendants did not adequately protect their Sensitive Information, Plaintiff and members of the Class would not have entrusted Defendants with their Sensitive Information.

115. Defendants' various violations and their failure to comply with applicable laws and regulations constitutes negligence *per se*.

116. As a direct and proximate result of Defendants' negligence per se, Plaintiff and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of Sensitive Information; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Sensitive Information, entitling them to damages in an amount to be proven at trial.

117. Additionally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their Sensitive Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants' fails to undertake appropriate and adequate measures to protect their Sensitive Information in their continued possession.

COUNT III
Breach of an Implied Contract
Against Defendant UC Health
(On Behalf of Plaintiff and the Class)

118. Plaintiff realleges all previous paragraphs as if fully set forth below.

119. Plaintiff and the Class delivered their Sensitive Information to Defendant UC Health as part of the process of obtaining treatment and services provided by UC Health.

120. Plaintiff and Class Members entered into implied contracts with Defendant UC Health under which Defendant agreed to safeguard and protect such information and to timely and

accurately notify Plaintiff and Class Members if and when their data had been breached and compromised. Each such contractual relationship imposed on Defendant an implied covenant of good faith and fair dealing by which Defendant was required to perform its obligations and manage Plaintiff's and Class Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendant.

121. In providing their Sensitive Information, Plaintiff and Class Members entered into an implied contract with Defendant UC Health whereby Defendant, in receiving such data, became obligated to reasonably safeguard Plaintiff's and the other Class Members' Sensitive Information.

122. In delivering their Sensitive Information to Defendant UC Health, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard that data.

123. Plaintiff and the Class Members would not have entrusted their Sensitive Information to Defendant UC Health in the absence of such an implied contract.

124. Defendant UC Health accepted possession of Plaintiff's and Class Members' Sensitive Information.

125. Had Defendant UC Health disclosed to Plaintiff and Class Members that Defendants did not have adequate computer systems and security practices to secure consumers' Sensitive Information, Plaintiff and members of the Class would not have provided their Sensitive Information to Defendant.

126. Defendant UC Health recognized that consumer's Sensitive Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and Class Members.

127. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant UC Health.

128. Defendant UC Health breached the implied contract with Plaintiff and Class Members by failing to take reasonable measures to safeguard its data.

129. Defendant UC Health breached the implied contract with Plaintiff and Class Members by failing to promptly notify them of the access to and exfiltration of their Sensitive Information.

130. As a direct and proximate result of the breach of the contractual duties, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' Sensitive Information; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Sensitive Information; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendants promised when Plaintiff and the proposed class entrusted Defendants with their Sensitive Information; and (h) the continued and substantial risk to Plaintiff's and Class Members' Sensitive Information, which remains in the Defendants' possession with inadequate measures to protect Plaintiff's and Class Members' Sensitive Information.

Count IV
Breach of Contract
Against Defendant Diligent
(On Behalf of Plaintiff and the Class)

131. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

132. Defendant Diligent entered into various contracts with its clients, including

healthcare providers, to provide software services to its clients.

133. These contracts are virtually identical to each other and were made expressly for the benefit of Plaintiff and the Class, as it was their confidential medical information that Defendant Diligent agreed to collect and protect through its services. Thus, the benefit of collection and protection of the Sensitive Information belonging to Plaintiff and the Class were the direct and primary objective of the contracting parties.

134. Defendant Diligent knew that if it were to breach these contracts with its healthcare provider clients, the clients' consumers, including Plaintiff and the Class, would be harmed by, among other things, fraudulent misuse of their Sensitive Information.

135. Defendant Diligent breached its contracts with its clients when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiff's and Class Members' Sensitive Information.

136. As reasonably foreseeable result of the breach, Plaintiff and the Class were harmed by Defendant Diligent's failure to use reasonable data security measures to store their Sensitive Information, including but not limited to, the actual harm through the loss of their Sensitive Information to cybercriminals.

137. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

138. Plaintiff realleges all previous paragraphs as if fully set forth below.

139. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

140. Plaintiff and members of the Class conferred a benefit upon Defendants in providing the Sensitive Information to Defendants.

141. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiff and the Class. Defendants also benefited from the receipt of Plaintiff's and the Class's Sensitive Information, as this was used to facilitate the treatment, services, and goods it sold to Plaintiff and the Class.

142. Under principals of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiff and the Class's Sensitive Information because Defendants failed to adequately protect their Sensitive Information. Plaintiff and the proposed Class would not have provided their Sensitive Information to Defendants had they known Defendants would not adequately protect their Sensitive Information.

143. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT VI
Violation of Colorado Consumer Protection Act
Colo. Rev. Stat. § 6-1-101, *et seq.*
(On Behalf of Plaintiff and the Colorado Subclass)

144. Plaintiff realleges all previous paragraphs as if fully set forth below.

145. Both Defendants qualify as a "person" under § 6-1-102(6) of the Colorado Consumer Protection Act ("Colorado CPA"), Colo. Rev. Stat. § 6-1-101, *et seq*.

146. Plaintiff and the Subclass provided and/or entrusted confidential Sensitive Information to Defendants, which Defendants collected, stored, and maintained.

147. Defendants are engaged in, and their acts and omissions affect, trade and commerce. Defendants' relevant acts, practices and omissions complained of in this action were

done in the course of Defendants' business of marketing, offering for sale, and selling goods and services throughout the United States.

148. In the conduct of their business, trade, and commerce, Defendants engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the provision or sale of services to consumers. Plaintiff and the Subclass furnished or purchased these services. Plaintiff and the Subclass are actual or potential consumers as defined by Colo. Rev. Stat § 6-1-113(1), *et seq*.

149. In the conduct of their business, trade, and commerce, Defendants collected and stored highly personal and private information, including Sensitive Information belonging to Plaintiff and the Subclass.

150. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard the Sensitive Information of Plaintiff and the Subclass and that the risk of a data breach was highly likely and/or that the risk of the data breach being more extensive than originally disclosed was highly likely.

151. Defendants should have disclosed this information regarding their computer systems and data security practices because Defendants were in a superior position to know the true facts related to their security practices, and Plaintiff and the Subclass could not reasonably be expected to learn or discover the true facts.

152. As alleged herein this Complaint, Defendants engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and the furnishing of debt collection and payment services to consumers in violation of the Colorado Consumer Protection Act, including but not limited to the following:

a. failing to adequately secure consumer's names and Social Security numbers;

b. failing to maintain adequate computer systems and data security practices to safeguard consumer's Sensitive Information;

c. failing to disclose the material information, known at the time of the transaction – collection and retention of consumer Sensitive Information– that their computer systems would not adequately protect and safeguard consumers' Sensitive Information;

d. inducing consumers to use Defendants' services by failing to disclose, and misrepresenting the material fact that Defendants' computer systems and data security practices were inadequate to safeguard their consumers' Sensitive Information from theft.

153. By engaging in the conduct delineated above, Defendants violated the Colorado Consumer Protection Act by, among other things:

a. omitting material facts regarding the goods and services sold;

b. omitting material facts regarding the security of the transactions between Defendants and consumers;

c. omitting material facts regarding the security of the transactions between Defendants and consumers who furnished or entrusted their Sensitive Information;

d. misrepresenting material facts in the furnishing or sale of products, goods or services to consumers;

e. engaging in conduct that is likely to mislead consumers acting reasonably under the circumstances;

f. engaging in conduct which creates a likelihood of confusion or of misunderstanding;

g. engaging in conduct with the intent to induce consumers to use Defendants' service;

h. unfair practices that caused or were likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers; and/or

i. other unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices to be shown at trial.

154. Defendants systemically engaged in these deceptive, misleading, and unlawful acts and practices, to the detriment of Plaintiff and the Subclass.

155. Defendants' actions in engaging in the conduct delineated above were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and the Class.

156. As a direct result of Defendants' violation of the Colorado Consumer Protection Act, Plaintiff and the Subclass have suffered actual damages, including but not limited to: (i) the loss of the opportunity how their Sensitive Information is used; (ii) the compromise, publication, and/or theft of their Sensitive Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Sensitive Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports;

(vi) the continued risk to their Sensitive Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect that Sensitive Information; and (viii) present and future costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the Sensitive Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Subclass.

157. As a result of Defendants' violation of the Colorado Consumer Protection Action, Plaintiff and the Subclass are entitled to, and seek, injunctive relief, including, but not limited to:

a. Ordering that Defendants engage third-party security auditors/penetration testers as well as experienced and qualified internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendants engage third-party security auditors and experienced and qualified internal security personnel to run automated security monitoring;

c. Ordering that Defendants audit, test, and train their security personnel regarding new or modified procedures;

d. Ordering that Defendants segment data by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Ordering that Defendants purge, delete, and destroy in a reasonably secure manner consumers' data not necessary for their provision of services;

f. Ordering that Defendants conduct regular database scanning and securing checks;

g. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and,

h. Ordering Defendants to meaningfully educate their consumers about the threats they face as a result of the loss of their Sensitive Information to third parties, as well as the steps consumers must take to protect themselves.

158. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices of Defendants alleged herein, Plaintiff and the Subclass seek relief under Colo. Rev. Stat. § 6-1-113, including, but not limited to, the greater of actual damages, statutory damages, or treble damages for bad faith conduct, injunctive relief, attorneys' fees and costs, as allowable by law.

PRAYER FOR RELIEF

Plaintiff and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendants from further deceptive practices and making untrue statements about the Data Breach and the stolen Sensitive Information;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff hereby demand that this matter be tried before a jury.

Date: March 22, 2023

Respectfully submitted,

By: /s/ James Bilsborrow
James Bilsborrow
WEITZ & LUXENBERG, PC
700 Broadway
New York, NY 10003
Telephone: (212) 558-5500
jbilsborrow@weitzlux.com

TURKE & STRAUSS LLP
Samuel J. Strauss*
Raina Borrelli*
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
sam@turkestrauss.com
raina@turkestrauss.com

Attorneys for Plaintiff and Proposed Class

***** to be admitted *pro hac vice*